Cassandra Crossing/ Kilroy e la Botnet

(223)—Il takeover sulla botnet Coreflood puo' essere chiamato un atto di cyberwar. O, più politically correct, una missione di…

Cassandra Crossing/ Kilroy e la Botnet



Figure 1:

(223)—Il takeover sulla botnet Coreflood puo' essere chiamato un atto di cyberwar. O, più politically correct, una missione di cyber-pace?

29 aprile 2011— "Kilroy" è una leggenda di origini incerte, evolutasi negli anni, ma particolarmente viva durante e subito dopo la Seconda Guerra Mondiale. In quegli anni Kilroy era una specie di personalità collettiva dell'esercito USA, un immaginario soldato che lasciava la traccia del suo passaggio, particolarmente in luoghi importanti o dove erano avvenuti fatti curiosi.

Si favoleggia, ma questa è probabilmente davvero una leggenda, che durante la conferenza di Potsdam fosse stato preparata una stanza blindata ad uso esclusivo dei capi di stato, che Stalin fosse il primo ad entrarvi, ma che ne sia uscito subito dicendo "*Chi è questo Kilroy*?".

La recente notizia della distruzione della botnet Coreflood da parte dell'FBI ha fatto la prevista (ed invero un po' troppo bassa) parabola nella *notiziosfera.*

La questione, ridotta all'essenziale, è la seguente: un'agenzia del governo statunitense, l'FBI, su ordine di un giudice ha compromesso e (sperabilmente) distrutto la botnet Coreflood, una grande struttura di PC infetti e trasformati in zombie tramite la quale venivano commessi reati anche negli Stati Uniti.

Questa botnet, scoperta nell'oramai lontano 2003, era controllata da remoto tramite una struttura *CCC* (Comando, Controllo e Comunicazione) a più livelli, e permetteva ai suoi padroni di

rivendere servizi illegali a terzi, dall'invio di spam fino ad attacchi DDoS, e certamente molto altro ancora.

Infatti le botnet moderne sono dotate di architetture flessibili, e possono essere programmate da remoto inserendo sui PC infetti ulteriori software malevoli a piacere, tramite una tecnica simile a quella dei plugin per i browser.

Sono stati fatti alcuni commenti assai interessanti sull'azione che è stata eseguita, ed in particolare sui suoi aspetti legali.

Cassandra però non è stata colpita da quanto detto, ma da quanto ha intravisto: le pare infatti di aver notato, su un normale cybermuro sbrecciato dalla cyberbattaglia, proprio quel graffito "Kilroy was here".

E questa è stata solo l'anticipazione di un pensiero, cioè che la prima vera cyberbattaglia di una cyberguerra è stata oggi combattuta ed ora è divenuta storia.

Certo, tutti ricorderanno che sia stato il massiccio DDoS che ha colpito l'Estonia ad essere definito la prima cyberwar. Vero, ma in quel caso è mancato un elemento importante di una vera cyberwar, l'essenza "cyber" di almeno uno dei contendenti.

La questione estone alla fin fine è stata solo una scaramuccia politica basata su rancori storici antichi, del tutto terrestri: manca l'aura cyberpunk che si ritrova allo stato puro nel personaggio di Invernomuto di Neuromante. Non questa volta. Questa volta uno Stato ha combattuto contro dei bit.

Questa volta ha vinto lo Stato. L'essere del cyberspazio è morto, o forse è ridotto in uno stato comatoso da cui potrebbe anche risorgere, come in tanti B-movie accade.

Colpisce anche che questa scaramuccia abbia in comune con tanti eventi militari successivi alla Seconda Guerra Mondiale il fatto di essere una guerra mai dichiarata.

Le dichiarazioni di guerra prima di eventi militari sono infatti passate di moda nel complicato mondo moderno. Persino il Giappone fece precedere di poco l'attacco a sorpresa su Pearl Harbor da una embrionale dichiarazione di guerra: i dettagli fini di un fatto storico complesso non cambiano il fatto che, anche durante un attacco a sorpresa, una dichiarazione di guerra formale fosse considerata importante.

Sembra quindi di poter concludere che, anche in questo caso, non di una cyberguerra si è trattato ma di una "cybermissione di pace" nel cyberspazio.

E in effetti è vero: in questo caso erano certamente i buoni contro cattivi.

E' finita 1 a zero per i buoni e palla al centro. Ma i buoni faranno meglio a stare molto attenti in futuro.

Coreflood, l'essere cyber, non si aspettava di essere attaccato, i suoi padroni nemmeno: la prossima volta la storia, e magari anche il finale, potrebbero essere molto diversi.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

***Licenza d'utilizzo**: i contenuti di questo articolo, dove non diversamente indicato, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link.

By Marco A. L. Calamari on June 24, 2023.

Canonical link

Exported from Medium on August 27, 2025.